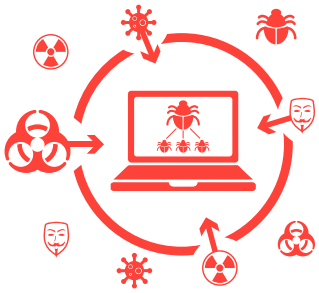
SOLUTION BRIEF

Add advanced threat protection to close your security gaps.

When the board asks, “How secure are we?,” what’s your response?



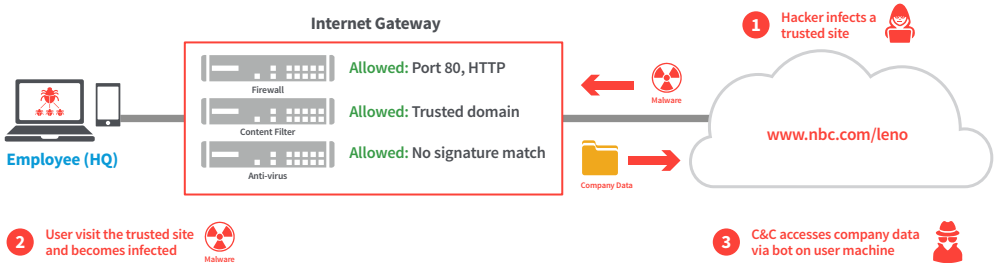
Find out in two minutes or less. Run the Zscaler™ Security Preview.

More than 2,800 enterprises layer Zscaler’s advanced threat protection over their traditional security appliances to close security gaps as part of their defense-in-depth strategy.

The changing IT and threat landscape

For years, enterprises have invested heavily in security appliances to establish a hard perimeter between their organizations and the internet to protect against threats. And, with each new threat type, the standard IT countermeasure was to deploy additional security appliances. This approach worked well when a majority of traffic was destined for applications in the data center, but today, the inverse holds true. Applications are now in the cloud and traffic patterns have followed.

Attackers are well aware of the changing IT landscape and have shifted their attack patterns accordingly. Attacks that were once targeted at the data center have shifted to the weakest link – the user – and they’re evading detection by employing techniques that exploit the shortcomings of security appliances.



IT and security professionals know what needs to be done to protect against this advancing threat landscape, but find themselves making tradeoffs between budget, level of inspection, and user experience.

Every hardware appliance you purchase is fundamentally limited in terms of capacity and functionality by the amount of processing power you can squeeze into the individual box. The deeper the level of inspection required the more boxes you need to buy and manage—and more boxes mean a slower end-user experience. This forces compromises in terms of what gets inspected and the depth of the inspection. Most enterprises sacrifice SSL inspection, since it can require eight times the number of appliances, and they often let traffic from content delivery networks (CDNs) go uninspected since it’s a pay-to-play service.

If you know these threats are real, but think they probably don't apply to you, find out for sure. A simple two-minute test using the Zscaler Security Preview will give you a picture of how secure you really are.

This is why over 2,800 enterprises are layering Zscaler's cloud security platform with advanced threat protection over their existing perimeter-based solutions.

40%

of Internet traffic crosses CDNs and goes uninspected.

Virtual Networking Index, Cisco

54%

of advanced threats hide behind SSL.

ThreatLabZ Research, Zscaler

Inspecting all traffic can require 8X more security appliances

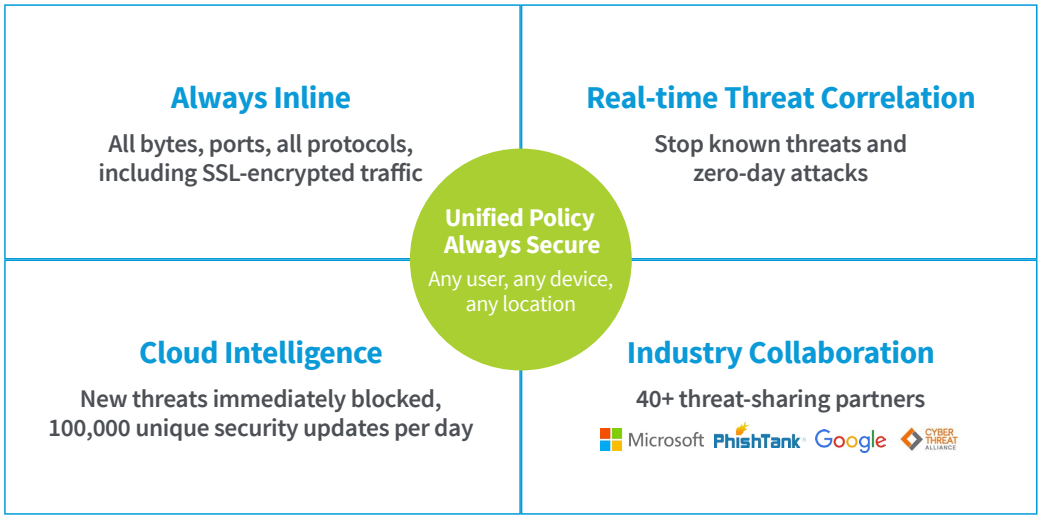
Close your security gaps by adding an extra layer in the cloud

Zscaler cost-effectively puts an extra layer of security and compliance between your existing infrastructure and the Internet, so it can find and block threats that are going undetected by your current security systems. Most proxies deployed today only do URL filtering and rely on additional appliances for security, including anti-virus.

Zscaler, in developing its cloud-based architecture, broke down all the functional components of a standalone proxy and re-imagined them—creating a distributed service that forms a single virtual proxy extending across more than 100 data centers. The Zscaler proxy-based architecture delivers superior protection over other types of security controls, because the entire file is downloaded, assembled, uncompressed, and scanned for malicious content before it reaches the end user or calls out to a command and control (C&C) server. All inspection is done at wire-rate performance with only microsecond latency.

Benefiting from the power of cloud computing, Zscaler's cloud security platform has the processing performance and scale to operate inline—inspecting every byte of traffic and performing real-time threat correlation using multiple techniques. The massive scale of the Zscaler global network provides unique insight into advanced and zero-day threats as they emerge.

Zscaler Advanced Threat Protection

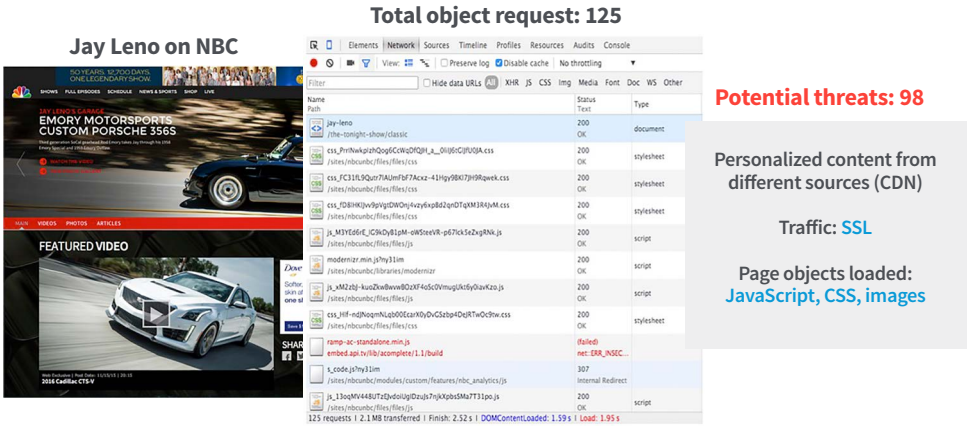


Zscaler inspects all content, all the time

Zscaler advanced threat protection begins by quickly validating that browser and plug-ins are compliant and then moves to full content inspection. It identifies malware buried deep within an otherwise legitimate page, so it doesn't slip through the cracks.

Using ByteScan technology, Zscaler efficiently inspects every byte of inbound and outbound traffic, including SSL, with only microsecond delay. Zscaler detects hidden iFrames, cross-site scripts, signs of phishing attempts, cookie stealing, and botnet communications to C&C servers.

All content is subjected to every level of inspection, always. That's important, because web pages are dynamically generated with personalized content consisting of hundreds of objects obtained from multiple sources. Each object poses a potential threat and must be considered untrusted regardless of source.



For each Web page served, Zscaler dynamically computes a PageRisk Index that takes into account the use of suspicious techniques, like JavaScript obfuscation and zero-pixel images, and correlates it with other factors, such as website location and reputation, to compute a risk score. The calculated score can then be compared to a predefined risk threshold to make an "allow or block" decision for the page or even page object. All of this is done on the fly without slowing the user experience.

Real-time threat correlation for comprehensive security

The Zscaler platform has the processing power to employ multiple threat prevention approaches and techniques in real time. And it goes much further, by correlating the information amassed across those techniques and turning it into actionable intelligence. Appliances were not designed to run as an integrated platform. They are purpose-built to perform their specific tasks and pass the traffic down the chain to the next appliance to perform its tasks. But correlation is critical to providing protection against rapidly changing and increasingly sophisticated threats.

REACTIVE	REAL-TIME	PREDICTIVE
Stop known threats	**Prevent zero-day attacks**	**Predict zero-day attacks**
Match destination or signature	Inline content inspection, all bytes, SSL	Behavioral analysis, machine learning, sandboxing
AV signature, blacklists, known botnets / C&C, known phishing	*Unknown botnet calls, unknown phishing, malicious JavaScript, XSS attacks*	*New malicious files, new malicious destinations*

Comprehensive security requires correlation across all three

Cloud intelligence: security in numbers

With more than 100 data centers around the world, Zscaler processes over 60 billion transactions at peak periods and detects more than 100 million threats. Out of the detected threats, less than one percent were blocked by anti-virus systems, meaning that Zscaler gains unique insight into advanced and zero-day threats—insight that helps us protect all users. That's because each time a new threat is detected by any one of our customers, it's immediately blocked for everyone. Knowledge obtained from the platform—machine learning—grows exponentially every time a new user is added.

Zscaler uses cloud intelligence to conduct 100,000 unique security updates every day, for the kind of protection no security appliance can touch.

99%

of threats blocked

by Zscaler would have evaded detection by traditional security appliances.

Zscaler security research stays ahead of threats

The Zscaler ThreatLabZ security research team continually mines billions of web transactions to identify new and emerging threats as they occur and deploys protection mechanisms to keep users safe. These efforts, along with feeds by more than 40 security partners, ensure the latest intelligence is being utilized at all times.

Policy deployment made simple

With Zscaler, you can define business policies once and those policies follow the user regardless of the device or location. As employees travel, their policies automatically move with them, and any policy change is immediately enforced worldwide on the very next web GET request. Common policies include:

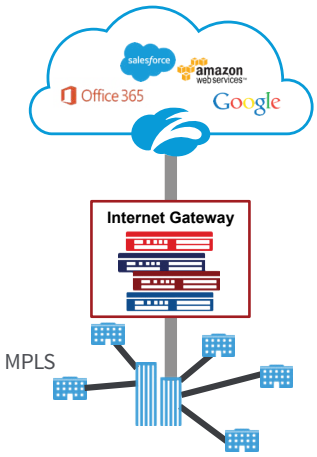
- Blocking peer-to-peer communications, like BitTorrent
- Blocking all traffic going to hostile countries
- Allowing .exe downloads only to IT at HQ

Run the Zscaler Security Preview. Then contact Zscaler.

The Zscaler Security Preview can tell you a lot about your security and compliance posture right now. And, once you've been able to identify gaps, Zscaler will help you close them.

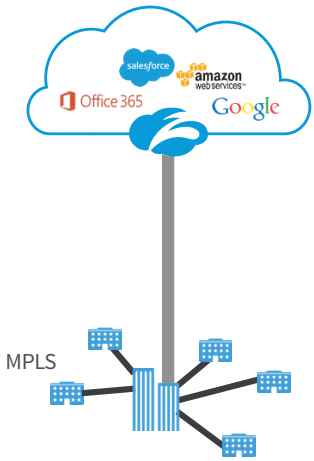
Getting started with Zscaler is simple, because there is no hardware or software to deploy or manage. Like Zscaler's 2,800+ enterprise customers, you will immediately enjoy increased security and compliance by making Zscaler your next hop to the internet after it transits your current security infrastructure. Almost all customers get started this way to improve security and overcome institutional resistance to change. Many are using Zscaler as the first step in becoming a cloud and mobile-first enterprise.

1 Add advanced threat protection – close gaps



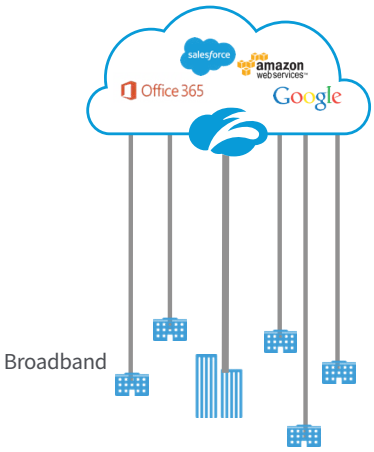
No policy or infrastructure changes

2 Break free from security appliances – simplify IT



Reduce costs and future-proof

3 Transform your security and network architecture



Fast user experience and optimized traffic flows

Learn more.

Advanced Threat Protection White Paper
Contact us: Talk to a cloud security specialist
Security Preview: How secure are you?

About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at **zscaler.com** or follow us on Twitter @zscaler.

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/company/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com